

#3

Customer No. 22,852
Attorney Docket No. 04329.2725

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:)
Atsushi SHIMBO et al.)
Serial No.: Not Yet Assigned) Group Art Unit: Not assigned
Filed: January 22, 2002) Examiner: Not assigned
For: MODULAR EXPONENTIATION)
CALCULATION APPARATUS)
AND MODULAR)
EXPONENTIATION)
CALCULATION METHOD)

Assistant Commissioner for Patents
Washington, DC 20231

Sir:

INFORMATION DISCLOSURE STATEMENT UNDER 37 C.F.R. § 1.97(b)

Pursuant to 37 C.F.R. §§1.56 and 1.97(b), applicants bring to the Examiner's attention the documents listed on attached Form PTO-1449. Copies of the listed documents are attached. Applicants respectfully request that the Examiner consider the documents listed on attached Form PTO-1449 and indicate that they were considered by making an appropriate notation on this form.

This Information Disclosure Statement is being filed with the above-referenced application.

This submission does not represent that a search has been made or that no better art exists and does not constitute an admission that each or all of the listed documents are material or constitute "prior art." If the Examiner applies any of the documents as prior art against any claim in the application and applicants determine

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

1c872 U.S. PRO
10/051276
01/22/02

that the cited documents do not constitute "prior art" under United States law, applicants reserve the right to present to the office the relevant facts and law regarding the appropriate status of such documents. Applicants further reserve the right to take appropriate action to establish the patentability of the disclosed invention over the listed documents, should one or more of the documents be applied against the claims of the present application.

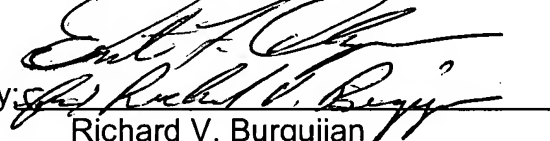
If there is any fee due in connection with the filing of this Statement, please charge the fee to our Deposit Account No. 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: January 22, 2002

By:


Richard V. Burgujian
Reg. No. 31,744

Enclosures
RVB/FPD/dvz

ERNEST F. CHAPMAN
Reg. No. 25,961

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

INFORMATION DISCLOSURE CITATION

Atty. Docket No.	04329.2725	Serial No.	
Applicant	Atsushi SHIMBO et al.		
Filing Date	January 22, 2002	Group:	Not assigned

1c872 U.S. PTO
10/051276
01/22/02

U.S. PATENT DOCUMENTS							
Examiner Initial*		Document Number	Issue Date	Name	Class	Sub Class	Filing Date If Appropriate

FOREIGN PATENT DOCUMENTS							
		Document Number	Publication Date	Country	Class	Sub Class	Translation Yes or No

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)	
	KAWAMURA, S. et al., "Cox-Rower Architecture for Fast Parallel Montgomery Multiplication", Eurocrypt 2000, LNCS 1807, pp.523-538, May 2000.
	Posch, K. et al., "Modulo Reduction in Residue Number Systems", IEEE Transactions on Parallel and Distributed Systems, Vol. 6., No. 5, pp.449-451, May 1995.
	Quisquater, J. J. et al., "Fast Decipherment Algorithm For RSA Public-Key Cryptosystem", Electronics Letters, Vol. 18, No. 21, pp. 905-907,(1982).
Examiner	Date Considered
*Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	
Form PTO 1449 Patent and Trademark Office - U.S. Department of Commerce	